IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

SOUTHWEST AIRLINES CO.,	§	
	§	
Plaintiff,	§	
	§	
v.	§	Case No. 3:21-cv-00098
	§	
KIWI.COM, INC., and KIWI.COM S.R.O.,	§	
	§	
	§	
Defendants.	§	

DEFENDANTS' BRIEF IN SUPPORT OF MOTION TO DISMISS CFAA CLAIM

TABLE OF CONTENTS

INDEX OF AUTHORITIES

CASES

STATUTES AND RULES

OTHER AUTHORITIES

INTRODUCTION

On June 3, 2021, the U.S. Supreme Court issued its opinion in *Van Buren v. United States*, holding that the concept of "authorization" embedded in the provisions of the Computer Fraud and Abuse Act (CFAA) must be construed narrowly as a binary "gates-up-or-gates-down inquiry." 141 S.Ct. 1648, 1658-59 (2021). This authoritative interpretation of the CFAA makes plain that violating website terms of service does not constitute a violation of federal law. Rather, under both the "without authorization" and "exceeds authorized access" prongs of the CFAA provisions at issue, *Van Buren* instructs that access—whether to a particular computer or a particular resource on a computer—is authorized, within the CFAA's meaning, if such access is permitted in at least one circumstance, even though the particular access complained of did not occur in such circumstances. If access is permitted for personal use, it is also authorized under the CFAA even if for commercial purposes. If information can be accessed manually, accessing it via automation is authorized under the CFAA to the same extent. Thus, unless the accessed computer or resource is entirely "off limits," *id.* at 1662, access, even in violation of terms of service, does not constitute a violation of the CFAA.

Van Buren dooms the CFAA claim that plaintiff Southwest Airlines Co. seeks to raise here. The foundation of that claim is that defendants Kiwi.com, Inc. and Kiwi.com s.r.o. (collectively, Kiwi.com) accessed a website Southwest made publicly available to all comers via the Internet but, in doing so, violated the unilateral Terms & Conditions that purportedly govern the use of that site. Southwest's own allegations plead it outside the narrow CFAA ambit that *Van Buren* circumscribes. Access to an unsecured public website cannot be "without authorization" by definition; the very act of making such a site available provides authorization to everyone with an Internet connection. And access to that website for a purpose deemed improper or in a manner or circumstance that violates restrictions imposed by terms of service does not "exceed authorized

access," because under *Van Buren* such access is authorized irrespective of those terms and conditions. Because Southwest cannot plead around these barriers, its claim must be dismissed.

Even if it somehow survived *Van Buren*'s abrogation of the key Fifth Circuit precedent on which it relies, Southwest's CFAA claim faces a further hurdle. Insofar as it arises under a provision of the CFAA requiring allegations of fraud and intent to defraud, Southwest must allege that fraud with particularity. Its live pleading does not even approach the specificity of "who, what, when, where, and how" that Rule 9 demands. Thus, at the very least, the CFAA claim must be dismissed in part.

STANDARDS GOVERNING THIS MOTION

I. STANDARDS FOR PLEADING AND DISMISSAL UNDER RULES 8, 9, AND 12

Federal courts evaluate the sufficiency of a complaint under Rule 12 "accepting all well-pleaded facts as true and viewing those facts in the light most favorable to the plaintiff." *Meador v. Apple, Inc.*, 911 F.3d 260, 264 (5th Cir. 2018). "A motion for judgment on the pleadings under Rule 12(c) is subject to the same standard as a motion to dismiss under Rule 12(b)(6)." *Ackerson v. Bean Dredging LLC*, 589 F.3d 196, 209 (5th Cir. 2009).[1]

Under the Federal Rules, "a pleading must contain 'a short and plain statement of the claim showing that the pleader is entitled to relief.'" *Olivarez v. T-Mobile USA, Inc.*, 997 F.3d 595, 599 (5th Cir. 2021) (quoting FED. R. CIV. P. 8(a)(2)). While "the pleading standard Rule 8 announces does not require 'detailed factual allegations,'" it does demand more than "labels and conclusions." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007)). Thus, "a formulaic recitation of the elements of a cause of action will not do."

[1] Because it has already answered, Kiwi.com, Inc. moves to dismiss pursuant to Rule 12(c); because it has not, Kiwi.com s.r.o. moves for the same relief pursuant to Rule 12(b)(6). *See Young v. City of Houston*, 599 Fed. App'x 553, 554 (5th Cir. 2015).

Twombly, 550 U.S. at 555. Rather, to survive a motion to dismiss, the complaint must plead "enough facts to state a claim to relief that is plausible on its face." *Id.* at 570. Those "[f]actual allegations must be enough to raise a right to relief above the speculative level." *Id.* at 555. "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678. Conversely, "where the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct, the complaint has alleged—but not 'shown'—that the pleader is entitled to relief." *Id.* at 679 (quoting Rule 8(a)(2); cleaned up).

In contrast, "Rule 9(b) imposes a heightened pleading standard in cases where the plaintiff alleges fraud or mistake: particularity." *In re Life Partners Holdings, Inc.*, 926 F.3d 103, 116-17 (5th Cir. 2019). "[T]o properly allege fraud under Rule 9(b), the plaintiff must plead the who, what, when, where, and why as to the fraudulent conduct." *Id.* And although the Rule "allows scienter to be 'averred generally,' simple allegations that defendants possess fraudulent intent will not satisfy Rule 9(b)." *Dorsey v. Portfolio Equities, Inc.*, 540 F.3d 333, 339 (5th Cir. 2008). Rather, the plaintiff "must set forth *specific facts* supporting an inference of fraud." *Id.* (quoting *Melder v. Morris*, 27 F.3d 1097, 1102 (5th Cir. 1994)).

II. ELEMENTS OF CLAIMS UNDER 18 U.S.C. §1030

Count Five of Southwest's complaint invokes two substantive prohibitions under the CFAA, 18 U.S.C. §1030. The first, subsection (a)(2)(C), penalizes a person who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer." 18 U.S.C. §1030(a)(2)(C). The second, subsection (a)(4), applies to one who, "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the

intended fraud and obtains anything of value." *Id.* §1030(a)(4).[2] The CFAA provides a private right of action to "[a]ny person who suffers damage or loss by reason of a violation of this section," including subsections (a)(2)(C) and (a)(4), but "only if the conduct involves" one of five specified factors, including "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." *Id.* §1030(g), (c)(4)(A)(i)(I).

"Taking all of this together," to plead a civil claim for violation of subsection (a)(2)(C), a plaintiff must plausibly allege facts showing that "(1) Defendants intentionally accessed a computer; (2) the access was unauthorized or exceeded Defendants' authorized access; (3) through that access, Defendants thereby obtained information from a protected computer; and (4) the conduct caused loss to one or more persons during any one-year period aggregating at least $5,000 in value." *Royal Truck & Trailer Sales & Serv., Inc. v. Kraft*, 974 F.3d 756, 759 (6th Cir. 2020). Meanwhile, a civil claim based on subsection (a)(4) requires plausible factual allegations that the defendant "(1) accessed a 'protected computer,' (2) without authorization or exceeding such authorization that was granted, (3) 'knowingly' and with 'intent to defraud,' and thereby (4) 'furthered the intended fraud and obtained anything of value,' causing (5) a loss to one or more persons during any one-year period aggregating at least $5,000 in value." *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132 (9th Cir. 2009).

Common and essential to both theories of Southwest's CFAA claim is the assertion that Kiwi.com's access to Southwest's protected computer was either "without authorization" or "exceed[ed] authorized access." 18 U.S.C. §1030(a)(2), (a)(4). In addition, insofar as its claim

[2] In addition, subsection (a)(4) specifies further criteria regarding the "thing of value," barring any claim if "the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period." 18 U.S.C. §1030(a)(4); *see, e.g.*, *United States v. Willis*, 476 F.3d 1121, 1126 (10th Cir. 2007) (noting distinction between requirement of something "of value" under (a)(4) and mere "information" under (a)(2)(C)). Southwest makes no allegation showing that this element of its claim is satisfied.

arises under subsection (a)(4), Southwest must allege both a fraud on Southwest by Kiwi.com and the mens rea to support it. *Id.* §1030(a)(4). Southwest does not—and cannot—allege these essential elements of its CFAA claim; accordingly, the claim fails.

ARGUMENT

I. *VAN BUREN V. UNITED STATES* REJECTS THE BROAD INTERPRETATION OF THE CFAA PREVIOUSLY PREVAILING IN THIS CIRCUIT.

The Supreme Court's recent authoritative interpretation of the CFAA makes plain that violations of website terms of service do not give rise to liability. *Van Buren v. United States*, 141 S.Ct. 1648 (2021).[3] Because that is the entire foundation of Southwest's CFAA claim, it cannot survive.

Van Buren resolves a longstanding circuit split over the meaning and scope of "authorization" under the CFAA's prohibitions against accessing protected computers "without authorization" and "exceed[ing] authorized access" to such computers. Namely, is authorization an all-or-nothing affair, or is it circumstance-specific and so capable of being limited to access for certain purposes only? *Van Buren* provides the definitive answer to the long-running dispute on this point—"authorization," for purposes of both clauses, is either all or nothing, a purely "gates-up-or-down inquiry." *Id.* at 1658-59.

Van Buren arose from the prosecution of a corrupt Georgia police officer who sold an informant data from license-plate search inquiries performed for non-law enforcement purposes. *Id.* at 1653. The parties agreed Van Buren was not "without authorization" in accessing the license-plate database but disputed whether departmental policy precluding its access for "any improper purpose," including "any personal use," meant Van Buren had "exceed[ed] authorized access." *Id.* at 1653-54. The Court ruled he had not.

[3] For the Court's convenience, a copy of the Supreme Court's slip opinion in *Van Buren* is attached as Exhibit A.

Closely analyzing the CFAA's definition of "exceeds authorized access" as using authorized access "to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter," 18 U.S.C. §1030(e)(6), the Supreme Court directly confronted the choice between interpreting that phrase narrowly to refer "to information one is not allowed to obtain *by using a computer that he is authorized to access*" or broadly interpreting it as referring "to information one was not allowed to obtain *in the particular manner or circumstances in which he obtained it*." 141 S.Ct. at 1655. Observing that "'[s]o' is not a free-floating term that provides a hook for any limitation stated anywhere," *id.*, the Court accepted Van Buren's narrower interpretation as more harmonious with the text, structure, and legislative history of the CFAA. *See id.* at 1655-61.

Critically, the Court insisted that both the "exceeds authorized access" and "without authorization" phrases of the statute be interpreted to complement one another according to a single, consistent understanding of "authorization." "Without authorization" "protects computers themselves by targeting so-called outside hackers—those who 'access a computer without any permission at all.'" *Id.* at 1658 (quoting *LVRC Holdings*, 581 F.3d at 1133; alteration omitted). Meanwhile, "exceeds authorized access" "provide[s] complementary protection for certain information within computers," "targeting so-called inside hackers—those who access a computer with permission, but then 'exceed the parameters of authorized access by entering an area of the computer to which that authorization does not extend." *Id.* (quoting *United States v. Valle*, 807 F.3d 508, 524 (2d Cir. 2015); alteration omitted). This account of the CFAA's key phrases "makes sense of the statutory structure because it treats the [two] clauses consistently." *Id.* Accordingly, "liability under both clauses stems from a gates-up-or-down inquiry—one either can or cannot

access a computer system, and one either can or cannot access certain areas within the system." *Id.* at 1658-59.[4]

The other crucial thread in *Van Buren* is the Court's patent alarm that the circumstance-specific understanding of "authorization" is significantly overbroad, particularly if that concept were defined by private arrangements dictated by computer owners, like website terms of use. If the CFAA "criminalizes every violation of a computer-use policy, then millions of otherwise law-abiding citizens are criminals"—a result Congress did not intend. *Id.* at 1661. Moreover, because the CFAA "prohibits only unlawful information 'access,' not downstream information 'misuse,'" whereas "purpose-based limits on access are often designed with an eye toward information misuse" and "can be expressed as either access or use restrictions," *Van Buren* rejects a reading of the CFAA that allows the scope of its prohibitions to be "controlled by the drafting practices of private parties." *Id.* at 1662.

In a passage directly applicable to this case, *Van Buren* effectively forecloses the CFAA claim Southwest asserts here:

> [C]onsider the Internet. Many websites, services, and databases—which provide 'information' from 'protected computers,' §1030(a)(2)(C)—authorize a user's access only upon his agreement to follow specified terms of service. If the 'exceeds authorized access' clause encompasses violations of circumstance-based access restrictions on employers' computers, it is difficult to see why it would not also encompass violations of such restrictions on website providers' computers."

[4] Notably, in adopting this parallel construction of the two phrases as stating categorical tests, *Van Buren* expressly rejects both an inconsistent approach to interpreting them ("the Government proposes to read the first phrase 'without authorization' as a gates-up-or-down inquiry and the second phrase 'exceeds authorized access' as one that depends on the circumstances") and a consistent, though circumstance-specific, interpretation of both ("the dissent would read both clauses . . . to require a circumstance-specific analysis"). *Id.* at 1659 & n.10. As the dissent makes clear, the *Van Buren* majority holding is that, "[s]o long as a person is entitled to use a computer to obtain information in at least *one* circumstance, this statute does not apply even if the person obtains data outside that circumstance." *Id.* at 1663 (Thomas, J., dissenting). "In effect," the CFAA applies "only when a person is 'not entitled *under any possible circumstance* so to obtain' information." *Id.* at 1663-64 (alterations omitted).

Id. at 1661. Because the CFAA does *not* adopt the circumstance-specific conception of "authorization," it does not "criminalize everything from embellishing an online dating profile to using a pseudonym on Facebook." *Id.* Likewise, it does not criminalize—or provide a private right of action against—commercial use of otherwise publicly available information or access via automated scripting, rather than through an individual's browser, simply because such limitations are stated in a website's terms of use.

In sum, *Van Buren* "settles that the CFAA is fundamentally a trespass statute," one whose "basic wrong is bypassing a closed gate, going where you're not supposed to go." Orin Kerr, *The Supreme Court Reins in the CFAA in* Van Buren, THE VOLOKH CONSPIRACY (Jun. 9, 2021), https://bit.ly/3gtEdOF. According to *Van Buren*, the CFAA "does not make it a crime to break a promise online," and it "does not make it a crime to violate terms of service." *Id.* And because it does not criminalize such conduct, it does not provide a civil claim against it either. 18 U.S.C. §1030(g).

Van Buren unequivocally rejects the broad interpretation of the CFAA that serves as the basis of Southwest's CFAA claim here. In contrast to now-abrogated decisions like *United States v. John*, 597 F.3d 263 (5th Cir. 2010), *Van Buren* forecloses the contract-based understanding of "authorization" under the CFAA that would "criminalize[] every violation of a computer-use policy." *Glam & Glits Nail Design, Inc. v. #NotPolish, Inc.*, 2021 WL 2317410, at *8 (S.D. Cal. June 7, 2021) (dismissing CFAA claim in light of *Van Buren*). Southwest previously highlighted the split between, on the one hand, Fifth Circuit precedents interpreting the CFAA like *John* and, on the other, decisions adopting the correct, narrow interpretation of the statute, suggesting that this Court would err if it did not follow *John*'s now-rejected broad interpretation. *E.g.*, Dkt. No. 34 at 1-2 & nn. 5-6. Now, however, "[t]he Supreme Court has spoken." *Glam & Glits*, 2021 WL

2317410. And it adopted a construction of the CFAA under which mere violations of a website's terms of use "cannot establish liability." *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067 (9th Cir. 2016), *cert. denied*, 138 S.Ct. 313 (2017); *accord Van Buren*, 141 S.Ct. at 1661-62.

Southwest's claim inexorably rises or falls on the validity of such terms-of-use violations as the basis for liability under the CFAA. *Van Buren* establishes beyond cavil that such violations cannot supply the basis for liability. 141 S.Ct. at 1661. Accordingly, the Court need go no further to determine that Southwest has failed to state a claim.

II. SOUTHWEST'S CFAA COUNT SHOULD BE DISMISSED FOR FAILURE TO STATE A CLAIM.

The understanding of the CFAA's substantive terms articulated in *Van Buren* is, on its face, sufficient ground for dismissal of Southwest's Count Five. Applying the interpretation of "authorization" adopted in *Van Buren* to Southwest's allegations further reinforces the point.

A. Kiwi.com Did Not Access Southwest's Servers "Without Authorization."

The foundation of the dispute alleged in Southwest's complaint is that Kiwi.com is accessing information resources that Southwest makes available to the public at large via the Internet, but over which Southwest seeks to maintain control via implementation of its Terms & Conditions. *E.g.*, FAC ¶¶2-3. Indeed, Southwest's complaint affirmatively alleges the global availability of its information via the Internet: "Southwest makes its website and the proprietary contents available for consumers' use subject to the Terms & Conditions." *Id.* ¶33. Likewise, it acknowledges that anyone on the Internet can access its information via that website: "Southwest's fares and flight schedules are proprietary. Although they are published openly on the internet, they are subject to specific use restrictions and may not be republished or used for commercial purposes without Southwest's express permission." *Id.* ¶32. It is thus an inescapable fact of this dispute, confirmed by Southwest's own allegations, that the information it seeks to control is publicly available.

As *Van Buren*'s adoption of the conception of "authorization" as a "gates-up-or-down inquiry" necessarily corroborates, 141 S.Ct. at 1658-59, "access is not 'without authorization' if it is for publicly available content," because "information open to the public is not the kind of access that the CFAA was designed to prevent." *Motogolf.com, LLC v. Top Shelf Golf, LLC*, __ F.3d __, 2021 WL 1147149, at *4 (D. Nev. Mar. 25, 2021); *accord, e.g.*, *Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am.*, 648 F.3d 295, 304 (6th Cir. 2011) (use of "unprotected public communications systems," like the phone network or "an unprotected website," precludes any allegation of access "without authorization," because systems "open to the public" authorize use by anyone) (cited by *Van Buren*, 141 S.Ct. at 1658); *Cvent, Inc. v. Eventbrite, Inc.*, 739 F.Supp.2d 927, 932-33 (E.D. Va. 2010) (rejecting claim that access was unauthorized, notwithstanding terms of service barring any site access by competitors, because "the entire world was given unimpeded access to Cvent's website," "the data which Eventbrite is alleged to have stripped from Cvent's website is publicly available on the Internet," and "Eventbrite was thus authorized to access it"). The CFAA's "authorization" concept divides the Internet "into at least two realms—*public* websites (or portions of websites) where no authorization is required and *private* websites where permissions must be granted for access." *Sandvig v. Barr*, 451 F.Supp.3d 73, 85 (D.D.C. 2020). The statute's bar on access "without authorization" applies only when "transitioning from a public area of the Internet to a private, permission-restricted area," thus "requiring some form of authentication before a viewer is granted access." *Id.* at 86.

Here, Southwest affirmatively alleges that its fare and flight information are "published openly on the internet" and that it relies on "mak[ing] its website and the proprietary contents available subject . . . to the Terms & Conditions" in order to "protect the security of its website and ensure normal operations." FAC ¶¶32-33. But as in *Cvent* and similar cases, Southwest does

not allege that its website "requir[ed] any login, password, or other individualized grant of access." 739 F.Supp.2d at 932. "Rather, anyone, including competitors" and anyone else with an Internet connection, "may access and search [Southwest's] information at will." *Id.* Under such circumstances, as a matter of law, Southwest cannot plausibly allege that Kiwi.com's access of such information was "without authorization." *See Sandvig*, 451 F.Supp.3d at 89 ("[A] user should be deemed to have 'accessed a computer without authorization' only when the user bypasses an authenticating permission requirement, or 'authentication gate,' such as a password restriction that requires a user to demonstrate 'that the user is the person who has access rights to the information accessed.'" (quoting Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1147, 1164 (2016)). Numerous district courts have reached the same conclusion—that no authorization is needed to access a site on the open Internet. *E.g.*, *Motogolf.com*, 2021 WL 1147149, at *5 (dismissing CFAA action for failure to state a claim based on "accessing a publicly accessible website"); *Miller v. 4Internet, LLC*, 471 F.Supp.3d 1085, 1090 (D. Nev. 2020) (same); *Koch Indus., Inc. v. Does*, 2011 WL 1775765, at *8 (D. Utah May 9, 2011) (rejecting "attempt to stretch the CFAA to the use of publicly available information on a website"); *Cvent*, 739 F.Supp.2d at 933 (dismissing CFAA claim based on accessing publicly available information because "Cvent's website, including its CSN database," was "not protected in any meaningful fashion by its Terms of Use or otherwise").

That conclusion is not affected by Southwest's cease-and-desist demands, for two reasons. First, while cease-and-desist letters may potentially serve to revoke authorization where effective access controls, like username and password restrictions, are in place, *e.g.*, *Power Ventures*, 844 F.3d at 1063, they have no such effect, vis-à-vis the CFAA, where information is "presumptively open to all comers" and no authorization is required, *id.* at 1067 n.2. "A computer owner cannot

both publish data to the world and yet keep specific users out just by expressing that intent." Kerr, *Norms of Computer Trespass*, at 1169. That is precisely the situation here.

Second, even presuming cease-and-desist communications might theoretically suffice to revoke authorization to access a public website, it is indisputable that Southwest's actual communications did not do so in this instance. In the series of emails and letters alleged in the complaint, Southwest repeatedly "notified Kiwi that it was violating the Terms & Conditions through, among other things, its unauthorized web scraping activity and offering a third-party product or service not authorized or approved by Southwest." FAC ¶¶56, 59, 65. In those communications, Southwest "demanded that Kiwi immediately cease and desist from (a) *extracting Southwest's flight and fare information* from the Southwest Website and its proprietary servers or websites; (b) *publishing Southwest fare information* on the kiwi.com website, through its mobile applications or elsewhere; and (c) *[making] use of the Southwest Registrations*." *Id.* ¶59 (emphases added); *accord* FAC Ex. B at 3, 4; FAC Ex. C at 6. Notably absent from any of these communications is language even arguably purporting to revoke Kiwi.com's authorization to access "the Southwest Website." *See, e.g.*, FAC ¶8 ("Southwest made it very clear . . . that Kiwi should immediately cease and desist *its ongoing unlawful, deceptive, and harmful conduct*." (emphasis added)).

Indeed, just the opposite is true—in demanding Kiwi.com's future compliance with Terms & Conditions purporting to govern access and use of southwest.com, Southwest's emails and letters implicitly acknowledge that Kiwi.com, like the rest of the world, remained free to access and use it. But to be "without authorization," a person must have "*no rights, limited or otherwise*, to access the computer in question." *Pulte Homes*, 648 F.3d at 304 (quoting *LVRC Holdings*, 581 F.3d at 1133). Conceding Kiwi.com's continued authorization to, for example, book Southwest

tickets for its own employees' use, *see* FAC ¶78, also concedes that Kiwi.com was not "without authorization."

The vision of the CFAA articulated in *Van Buren* necessarily clarifies that unsecured public websites like Southwest's, which require no permission to access, cannot be accessed "without authorization" by definition. *See, e.g.*, *Sandvig*, 451 F.Supp.3d at 85, 89 ("a website or portion of a website becomes 'private'" and so subject to CFAA protection "only if it is delineated as private through the use of a permission requirement of some sort"); *Cvent*, 739 F.Supp.2d at 932 (agreeing that, "[b]y definition," accessing information "publicly available on the Internet, without requiring any login, password, or other individualized grant of access" does not violate the CFAA); *cf. Sandvig v. Sessions*, 315 F.Supp.3d 1, 13 (D.D.C. 2018) ("[S]imply placing contractual conditions on accounts that anyone can create," as distinguished from "tak[ing] real steps to limit who can access [information]," "does not remove a website from the First Amendment protections of the public Internet."). And against the backdrop of such public availability, cease-and-desist communications are ineffective in revoking authorization for purposes of the CFAA. *Motogolf.com*, 2021 WL 1147149, at *5; *see* Kerr, *Norms of Computer Trespass*, at 1169. Moreover, because the cease-and-desist letters Southwest sent never "plainly put [Kiwi.com] on notice that it was no longer authorized to access [Southwest's] computers" at all, *Power Ventures*, 844 F.3d at 1067, they did not revoke Kiwi.com's authorization even if they theoretically could have. *See, e.g.*, *Miller*, 471 F.Supp.3d at 1090-91 (observing that cease-and-desist letter did not "plainly revoke Higbee or his law firm's authorization to access the website" and rejecting plaintiff's assertion that "telling the violating party to stop is sufficient" to make violating public sites' terms of service actionable under the CFAA); *see also NW Monitoring LLC v. Hollander*, 2021 WL 1424690, at *5 (W.D. Wash. Apr. 15, 2021) (the CFAA "requires *express* revocation of

previously granted authorization"); *Power Ventures*, 844 F.3d at 1067 n.2. Either way, the cease-and-desist communications Southwest alleges do not revive its invalid assertion that Kiwi.com's access to Southwest's servers was "without authorization."

B. Kiwi.com Did Not "Exceed Authorized Access" to Southwest's Servers.

Because Kiwi.com's access to Southwest's servers was not "without authorization," it could violate the CFAA only if it instead "exceed[ed] authorized access." 18 U.S.C. §1030(a)(2)(C), (a)(4). But *Van Buren* dictates that the scope of Kiwi.com's "authorization" for purposes of that inquiry is defined not by the purpose-based and other circumstance-specific restrictions stated in Southwest's Terms & Conditions, but by whether the information resources Kiwi.com accessed were wholly "off limits." 141 S.Ct. at 1662. The allegations of Southwest's complaint confirm they were not—Kiwi.com accessed flight and fare information and made flight arrangements using the same publicly exposed resources that it would have accessed by loading southwest.com in a web browser and buying a ticket. Accordingly, in light of *Van Buren*'s clear rule, Kiwi.com did not exceed its authorized access to Southwest's servers as a matter of law.

Van Buren holds that "an individual 'exceeds authorized access'" as defined by the CFAA "when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him." *Id.* The inquiry is categorical—"gates-up-or-down," meaning "one either can or cannot access certain areas within the system"—and asks whether access to a resource or data is *ever* authorized, irrespective of "the particular manner or circumstances" of a given instance of access. *Id.* at 1655, 1658-59. As Justice Thomas's dissent pithily puts it, *Van Buren* reads the CFAA "to apply only when a person is not entitled *under any possible circumstance* so to obtain information." *Id.* at 1664 (Thomas, J., dissenting; cleaned up). Thus, "[s]o long as a person is entitled to use a computer

to obtain information in at least *one* circumstance, this statute does not apply even if the person obtains the data outside that circumstance." *Id.* at 1663.

"The only question," *Van Buren* thus instructs, "is whether [Kiwi.com] could use [Southwest's] system to retrieve" the information it obtained—fare and flight data and booked flight reservations. *Id.* at 1662 (maj. op.). Southwest's complaint expressly alleges that Kiwi.com could and did do so. Whether it did so in violation of the purpose-based or other circumstance-specific use restrictions stated in the Terms & Conditions is irrelevant. *See id.* at 1654-55 (rejecting interpretation of "exceeds authorized access" that "refer[s] to information one was not allowed to obtain *in the particular manner or circumstances in which he obtained it*"); *accord, e.g.*, *Sandvig v. Sessions*, 315 F.Supp.3d at 26-27 ("The focus is on *what* information [users] access, not on why they wish to access it, the manner in which they use their authorization to access it, or what they hope to do with it.").

Numerous allegations in the complaint confirm the point. For example, with respect to its "proprietary" flight and fare information, Southwest pleads that it "makes its website *and the proprietary contents* available for consumers' use subject to the Terms & Conditions." FAC ¶33 (emphasis added). It details how, "[b]efore February 24, 2021," Kiwi.com allegedly "was using automated web-scraping script to access the 'front end' of Southwest.com." FAC ¶76. "Kiwi's 'bots,'" Southwest alleges, "accessed Southwest.com from the front end *in the same way that an individual user does*. . . . The automated request that the bot sent to Southwest.com *was the same as if an individual user had clicked 'Purchase.'*" *Id.* (emphases added). Thus, Southwest's allegations acknowledge that (1) Kiwi.com accessed information and resources available to all users of its site and (2) Kiwi.com did so in a manner indistinguishable in form and scope from any other user's interactions with the site.

Most damning, and under *Van Buren* dispositive of the "exceeds authorized access" inquiry all on its own, Southwest concedes that, on multiple occasions, "an individual user from Kiwi manually accessed and purchased tickets through the front end of Southwest.com." FAC ¶78. Just as Officer Van Buren did not exceed authorized access as a matter of law because, having "accessed the law enforcement database system with authorization," he "could use the system to retrieve license-plate information" under other circumstances than the ones that led to him being criminally charged, *Van Buren*, 141 S.Ct. at 1662, Southwest's affirmative allegation that Kiwi.com was allowed to access the public Southwest website, view flight and fare information, and book multiple tickets confirms irrefutably that it "is entitled to use a computer to obtain [such] information in at least *one* circumstance," meaning the CFAA's prohibition on "exceed[ing] authorized access" "does not apply even if the person obtains the data outside that circumstance." *Id.* at 1663 (Thomas, J., dissenting). Because Kiwi.com is authorized to obtain the information when using southwest.com "manually," FAC ¶78, any gates protecting that information are up, and Kiwi.com does not violate the CFAA by obtaining that information via automated script or by accessing it for the purpose of commercial use, notwithstanding the Terms & Conditions' bars on doing so. *Van Buren*, 141 S.Ct. at 1658-59. In light of *Van Buren*, as a matter of law, Southwest's allegations conclusively disprove that Kiwi.com "exceed[ed] authorized access."

III. ALTERNATIVELY, INSOFAR AS IT ARISES UNDER CFAA SUBSECTION (a)(4), SOUTHWEST'S CLAIM SHOULD BE DISMISSED FOR FAILING TO ALLEGE FRAUD WITH THE REQUISITE PARTICULARITY.

Federal Rule of Civil Procedure 9 commands that, "[i]n alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake," though intent and knowledge "may be alleged generally." FED. R. CIV. P. 9(b). Fraud is an essential element of claims arising under 18 U.S.C. §1030(a)(4), which must allege "intent to defraud" and "the intended fraud" in furtherance of which the protected computer was accessed. *LVRC Holdings*, 581 F.3d at

1132. Accordingly, "claims brought under §1030(a)(4) . . . need to be pled with particularity." *Villareal v. Saenz*, 2021 WL 1986831, at *7 (W.D. Tex. May 18, 2021). That conclusion follows because Rule 9(b)'s particularity prerequisite "quite plainly applies to section 1030(a)(4)'s requirement that the defendant's acts further the intended fraud." *Motorola, Inc. v. Lemko Corp.*, 609 F.Supp.2d 760, 765 (N.D. Ill. 2009); *accord, e.g.*, *Synopsys, Inc. v. Ubiquiti Networks, Inc.*, 313 F.Supp.3d 1056, 1072 (N.D. Cal. 2018).

Pursuant to Rule 9(b)'s dictate, "[a]t a minimum," Southwest must plead specific facts showing "the who, what, where, when, and how of the alleged fraud." *Colonial Oaks Assisted Living Lafayette, L.L.C. v. Hannie Dev., Inc.*, 972 F.3d 684, 689 (5th Cir. 2020). Southwest's first amended complaint fails to do so. *See* FAC ¶118 (generically reciting, in statutory language, that Kiwi.com's access "furthered the intended fraud"). Indeed, Southwest does not allege *any* details supporting its conclusory assertions of Kiwi.com's purported fraud on Southwest. Rather, its sole factual allegation in support of this element is itself wholly conclusory: "Kiwi knowingly and intentionally targets the Southwest Website to harvest Southwest's fare and pricing information for its own commercial benefit and without Southwest's authorization. Kiwi uses Southwest's information that is fraudulent, false or misleading, and that violates the Terms & Conditions of the Southwest Website." FAC ¶40. That is patently insufficient under this Court's and the Fifth Circuit's rigorous standards for pleading fraud. *See, e.g.*, *Williams v. WMX Techs., Inc.*, 112 F.3d 175, 177-78 (5th Cir. 1997) ("[T]he requirement for particularity in pleading fraud does not lend itself to refinement, and it need not in order to make sense. Directly put, the who, what, when, and where must be laid out *before* access to the discovery process is gratned."); *VeroBlue Farms USA, Inc. v. Wulf*, 465 F.Supp.3d 633, 653-56 (N.D. Tex. 2020) (decrying notice deficiencies inherent in "group pleading of fraud" and observing that merely "labeling a group as fraudsters—and then

seeking discovery to tighten the allegations after the fact—is [not] consistent with the Fifth Circuit's view of Rule 9's heightened pleading requirements"). Having thus tied its §1030(a)(4) claim to assertions of actual fraud, Southwest must plead them with particularity as Rule 9(b) requires. It has not done so, and that failure requires dismissal of its CFAA claim insofar as it arises under §1030(a)(4).

CONCLUSION

For the foregoing reasons, Kiwi.com respectfully requests that the Court dismiss Count Five of the first amended complaint with prejudice for failure to state a claim under the CFAA, 18 U.S.C. §1030. Alternatively, Kiwi.com respectfully requests that the Court dismiss Count Five insofar as it purports to arise under 18 U.S.C. §1030(a)(4) for failure to allege fraud with particularity as required by Rule 9(b).

Respectfully submitted,

/s/ Kieran McCarthy
Kieran McCarthy (*admitted pro hac vice*)
Colorado Bar No. 37933
Asa C. Garber (*admitted pro hac vice*)
Colorado Bar No. 48256
MCCARTHY GARBER LAW, LLC
501 S. Cherry Street #1100
Denver, Colorado 80246
(720) 504-5294
kieran@mccarthygarberlaw.com
asa@mccarthygarberlaw.com

Alexander Kerr (*admitted pro hac vice*)
Wyoming Bar No. 7-5782
MCCARTHY GARBER LAW, LLC
320 E. Broadway, Suite 2A
Jackson, Wyoming 83001
(970) 270-4718
alex@mccarthygarberlaw.com

Ryan P. Bates
Texas Bar No. 24055152
BATES PLLC
919 Congress Avenue, Suite 1305
Austin, Texas 78701
(512) 694-5268
rbates@batespllc.com

Benton Williams II
Texas Bar No. 24070854
BENTON WILLIAMS PLLC
100 Crescent Court, Suite 700
Dallas, Texas 75201
(214) 785-6205
(214) 785-6485 (fax)
bw@bentonwilliamspllc.com

Attorneys for Defendants
Kiwi.com, Inc. and Kiwi.com s.r.o.

CERTIFICATE OF SERVICE

I hereby certify that, on the 22nd day of June, 2021, I served a copy of the foregoing Brief in Support of Motion to Dismiss CFAA Claim on the attorneys of record for all parties via the Court's electronic filing system, as follows.

Michael C. Wilson
S. Wallace Dunwoody
Amanda K. Greenspon
Julie M. Christensen
MUNCK WILSON MANDALA, LLP
12770 Coit Road, Suite 600
Dallas, Texas 75251
mwilson@munckwilson.com
wdunwoody@munckwilson.com
agreenspon@munckwilson.com
jchristensen@munckwilson.com

Counsel for Plaintiff Southwest Airlines Co.

/s/ Ryan P. Bates
Ryan P. Bates